

Received & Inspected

FEB 18 2015

February 18, 2015

FCC Mail Room

Marlene H. Dortch, Secretary,  
Federal Communications Commission,  
445 12th Street SW, Suite TW-A325,  
Washington, DC 20554

DOCKET FILE COPY ORIGINAL

RE: **EB Docket No. 06-36**

Annual 64.2009(e) CPNI Certification for 2015 covering the prior calendar year 2014

1. Date filed: February 18, 2015
2. Name of company(s) covered by this certification: Quick Connect VoIP Inc.
3. Form 499 Filer ID: 826110
4. Name of signatory: Bruce Yuille
5. Title of signatory: President

This document consists of 2 pages, with the certification statement of officer on page 2.

6. Certification:

I, Bruce Yuille, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, record keeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken actions (*i.e.*, proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

The company has not received customer complaints in the past year concerning the unauthorized release of CPNI.

The company represents and warrants that the above certification is consistent with 47 C.F.R. § 1.17, which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed  [Signature of an officer, as agent of the carrier]

CERTIFICATION STATEMENT

No. of Copies rec'd  
List ABCDE

0+4

FEB 18 2015

FCC Mail Room

Quick Connect VoIP, Inc., is a small family owned interconnected VoIP service provider that provides voip and hosted Centrex like services to less than 100 business customers. Because we are so small, I personally supervise all employees on a daily basis. All employees are very experienced, having worked for VoIP for more than 5 years.

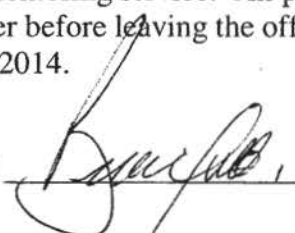
I have personally provided each employee with a copy of the CNPI rules and discussed same with them. VoIP does not solicit its customers to sell them anything. The selling was done when the customer signed a written service contract. VoIP does not generally call its customers unless to notify them about a potential service outage due to planned network maintenance or to up date them on repair or quality of service issues. Customers contract VoIP by either a phone call or email to service. I am on the customer serviced email distribution list and I receive copies of all customer e-mails and personally read them. Therefore I would know of any complaints about CNPI, and whether or not our employees violated any CNPI rules. If any violations occurred, they would be logged into an Excel Spreadsheet. In any event, the customer is verified against customer records before any action is taken.

VoIP does not solicit its customers by any means for any reason to sell them anything. Hence we do not possess any summary of marketing contacts with our customers because none have taken place. VoIP only responds to customer initiated requests and inquiries. All callers are verified against customer records or voice recognition from prior contacts over years of our business relationship, before any conversation about their services take place. VoIP has never received a customer complaint that it released CNPI to any unauthorized person.

Electronic call record detail is stored on secured servers that are only accessible by myself and the company's director of IT. Customer records are stored on office computers and in hard files.

Customer service records are only accessible within our company network by VoIP personnel when they are physically present in our office. We do not allow remote access into customer service computers. All network computer devices that use vendor software are updated on a weekly basis with any vendor patches released that week. Computers that are connected to the Internet use Linux based operating systems to thwart hackers. Hackers generally do not spend the time trying to find exploits in the Linux version that we use. VoIP created its own proprietary billing and customer service software. Same was written in a secure fashion to prevent against SQL injections, buffer overflows, and brute force attacks. Since hackers cannot hack a computer when it is not turned on, all office computers are turned off at the end of each business day. I periodical personally check the after hours computer status.

Our office doors are locked at all times, so that only authorized persons enter our office. Hard copies documents containing CNPI (service contracts and copies of relevant emails) are kept inside our locked office. After hours our office is monitored for intrusion and motion by a long standing third party mentoring service. All papers that contain any CNPI information is first shredded in the office shredder before leaving the office. No one gained unauthorized entry or access to hard copy CNPI during 2014.

Signed  [Signature of an officer, as agent of the carrier]